State of Indiana
Indiana Office of Technology

Information Resources Use Agreement (IRUA)

Information Resources are provided by the State to support the business of state government. The term "Information Resources" includes all state hardware, software, data, information, network, personal computing devices, phones, and other information technology. To use Information Resources, you agree to adhere to the provisions of this agreement, which are established to ensure security and inform you of the conditions of use.

1. Appropriate Use.

a. **Use for State Business.** I understand that Information Resources are to be used to conduct the business of state government. I understand that Information Resources may be used for *de minimis*, *i.e.*, limited, personal use that cannot reasonably be handled away from work. I shall minimize personal use of Information Resources.

b. **Approved Information Resources.** I shall only use Information Resources owned, licensed, or being evaluated by the State and shall not use personal or third party information resources, excluding cell phones and PDAs, at state facilities unless I have obtained prior written approval from the State Chief Information Security Officer (CISO).

c. **Protecting from Misuse & Damage.** I shall use care in protecting against unauthorized access, misuse, theft, damage, or unauthorized modification of Information Resources. I shall not leave a workstation without first ensuring it is properly secured from unauthorized access.

d. **Public Disclosure & Monitoring.** I understand that any information created, accessed, or stored on Information Resources, including my e-mail and my Internet use, may be subject to public disclosure. *The State reserves the right to monitor any and all use of Information Resources, including my e-mail and Internet use, and I have no right to and no expectation of privacy with respect to my use of Information Resources.*

2. **Prohibited Activities.** I understand that activities prohibited by this agreement may not be permitted without the prior written approval of the CISO. Prohibited activities include:

a. **Commercial & Politics.** I shall not use Information Resources to conduct business related to an outside, for profit, commercial activity. Unless permitted by law, I shall not use Information Resources to support any political party or candidate.

b. **Downloads.** I shall not install any software, including privately purchased or downloaded software such as screen savers, spyware, games, etc., without a legitimate state purpose. I shall not intentionally sustain high volume network traffic for non-business purposes hindering others use of the network or possibly increasing state costs.

c. **Inappropriate Material.** I shall not use Information Resources to access, upload, download, or distribute any jokes, comments, messages, or any other materials that are considered pornographic, obscene, sexually explicit, discriminatory, harassing, or defamatory, to employees or third parties, including but not limited to any content that might offend someone on the basis of age, gender, race, national origin, disability, or religion.

d. **Virus Protection.** I shall not disable virus protection for any reason and shall report malfunctioning virus protection software to the IOT Help Desk.

e. **Violation of Law.** I shall not use Information Resources to violate any law, including copyright or other intellectual property law. I shall not copy, share, or distribute software without authorization. I shall not reveal confidential information which may include but is not limited to: financial information, medical records, social security numbers, databases and the information contained therein.

f. **Chain Letters & Spam.** I shall not knowingly forward or respond to chain letters, pyramid selling schemes, marketing schemes, or unsolicited external commercial e-mail, commonly referred to as "spam."

g. **Unauthorized Use.** I shall not permit unauthorized users to use the Information Resources that the State has provided me. I shall promptly report any unauthorized use to my manager or the CISO.

h. **Access.** I shall not share confidential computer password(s) with any other person nor shall I use another person's confidential computer password(s). I shall not attempt to access information which I have no authorization to access. I shall connect to the state network only through approved services (e.g. – Citrix and VPN services are approved; a direct dial-up connection to a work PC modem is prohibited).

3. **Property of the State.** Information including but not limited to documents, software, files, and email, that I create, access, transmit, or store while using Information Resources are the State's property unless otherwise provided by contract.

4. **Violations & Uncertainty.** I shall report violations of this agreement to my manager or the CISO upon learning of such violations. If I am uncertain whether an activity is permissible, I will refrain from the activity and obtain authorization from my manager before proceeding.

5. **Disciplinary Action.** I am aware that my inappropriate use of Information Resources could result in disciplinary actions, up to and including immediate dismissal from employment, criminal prosecution where the act constitutes a violation of law and an action for breach of contract where applicable.

6. **Changes and additional information.** I understand this policy will be updated, that the State will make reasonable efforts to inform me of the changes, and that I am held accountable to abide by the current version posted at http://iot.in.gov/security/irua/. On this website I can also find IRUA clarifications and exceptions and answers to frequently asked questions.